PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Christine Cheng et al. Examiner: Ojo O. Oyebisi

Serial No.: 09/905,046 Group Art Unit: 3696

Filed: July 12, 2001 Docket: 2043.258US1

For: METHOD AND APPARATUS TO DETECT SUSPICIOUS TRANSACTION WITHIN A NETWORK-BASED AUCTION FACILITY

APPEAL BRIEF UNDER 37 CFR § 41.37

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Appeal Brief is presented in support of the Notice of Appeal to the Board of Patent Appeals and Interferences, filed on Herewith, from the Final Rejection of claims 1 - 40 of the above-identified application, as set forth in the Final Office Action mailed on February 14, 2008.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of $540.00 which represents the requisite fee set forth in 37 C.F.R. § 41.20(b)(2). The Appellants respectfully request consideration and reversal of the Examiner's rejections of pending claims.

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, EBAY INC, as evidenced by the assignment from inventors Christine Cheng, et al. recorded in the USPTO on July 12, 2001 on Reel 012006, starting at Frame 0526.

2. RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellant that will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

The present Application was filed on July 12, 2001 with claims 1 - 40. A Non-Final Office Action rejecting claims 1 - 40 was mailed on June 1, 2006. A Non-Final Office Action response was filed on October 27, 2006. A Final Office Action maintaining the rejection of claims 1 - 40 was mailed on January 29, 2007. A Final Office Action response was filed on March 29, 2007. An Advisory Office Action maintaining the rejection was mailed on April 10, 2007. A Request for Continued Examination was filed on April 30, 2007. A second Non-Final Office Action rejecting claims 1 - 40 was mailed on July 18, 2007. A second Non-Final Office Action response was filed on November 1, 2007. A Second Final Action maintaining the rejection of claims 1 - 40 was mailed on February 14, 2008. A second Final Office Action response was filed on May 13, 2008. An Advisory Office Action maintaining the rejection of claims 1 - 40 was mailed on June 9, 2008. A Pre-Appeal Brief request for review was filed on June 10, 2008. A decision on the Pre-Appeal Brief request for review was mailed on September 10, 2008 stating that the Application remains under Appeal. **Claims 1 - 40 stand rejected, remain pending, and are the subject of the present Appeal.**

4. STATUS OF AMENDMENTS

No amendments have been made subsequent to the Final Office Action mailed on February 14, 2008.

5. SUMMARY OF CLAIMED SUBJECT MATTER

INDEPENDENT CLAIM 1

Some aspects of the present inventive subject matter include, but are not limited to a method to detect fraudulent activities at a network-based transaction facility, the method comprising: causing a first identifier associated with a first user identity to be stored on a machine responsive to a first sales-related event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network (e.g., Fig. 6A, page 14, paragraph [0047], lines 6-15; e.g., Fig. 6C, page 15, paragraph [0049], lines 6-22); and detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine (e.g., Fig. 6B, page 14, paragraph [0048], lines 16-23; e.g., Fig. 6D, page 16, paragraph [0050], lines 1-18).

INDEPENDENT CLAIM 31

Some aspects of the present inventive subject matter include, but are not limited to a computer readable medium comprising instructions, which when executed on a processor, cause the processor to perform a method for detecting suspicious transactions made over a network-based transaction facility using a client machine, the method comprising: causing a first identifier associated with a first user identity to be stored on a machine responsive to a first sales-related event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network (e.g., Fig. 6A, page 14, paragraph [0047], lines 6-15; e.g., Fig. 6C, page 15, paragraph [0049], lines 6-22); and detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the

machine (e.g., Fig. 6B, page 14, paragraph [0048], lines 16-23; e.g., Fig. 6D, page 16, paragraph [0050], lines 1-18).

INDEPENDENT CLAIM 32

Some aspects of the present inventive subject matter include, but are not limited to a method for detecting suspicious transactions made with an Internet service facility from one computerized facility, the method comprising: causing a first identifier associated with a first user identity to be stored on a machine, the causing being responsive to a first sales-related event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network (e.g., Fig. 6A, page 14, paragraph [0047], lines 6-15; e.g., Fig. 6C, page 15, paragraph [0049], lines 6-22); and detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity, the detecting being responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine (e.g., Fig. 6B, page 14, paragraph [0048], lines 16-23; e.g., Fig. 6D, page 16, paragraph [0050], lines 1-18).

INDEPENDENT CLAIM 33

Some aspects of the present inventive subject matter include, but are not limited to a system to detect fraudulent activities at a network-based transaction facility, the system comprising:
an identifier processor to cause a first identifier associated with a first user identity to be stored on a machine responsive to a first sales-related event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network (e.g., Fig. 6A, page 14, paragraph [0047], lines 6-15; e.g., Fig. 6C, page 15, paragraph [0049], lines 6-22); and a first detection processor to detect a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine (e.g., Fig. 6B, page 14, paragraph [0048], lines 16-23; e.g., Fig. 6D, page 16, paragraph [0050], lines 1-18).

INDEPENDENT CLAIM 40

Some aspects of the present inventive subject matter include, but are not limited to a first means for causing a first identifier associated with a first user identity to be stored on a machine responsive to a first sales-related event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network (e.g., Fig. 6A, page 14, paragraph [0047], lines 6-15; e.g., Fig. 6C, page 15, paragraph [0049], lines 6-22); and a second means for detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine (e.g., Fig. 6B, page 14, paragraph [0048], lines 16-23; e.g., Fig. 6D, page 16, paragraph [0050], lines 1-18).

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

§102 Rejection of the Claims

Claims 1-6, 31-36 and 40 were rejected under 35 U.S.C. § 102(b) for anticipation by Trostle (U.S. 5,919,257; hereinafter "Trostle").

§103 Rejection of the Claims

Claims 7-8, and 37 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Trostle in view of Buchner et al (Discovering Internet marketing intelligence through online analytical web usage mining, ACM SIGMOD Record archive, Volume 27, Issue 4 December 1998, Pages: 54 - 61, Year of Publication: 1998, ISSN:0163-5808; hereinafter "Buchner").

Claims 9-19, and 38 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Trostle in view of Buchner and in further view of Miller (Michael Miller, The complete Idiot's Guide to Ebay Online Auctions, copyright July 1999; hereinafter "Miller").

Claims 20-21, and 39 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Trostle in view of Buchner and Miller and in further view of Smaha et al (U.S. 5,557,742; hereinafter "Smaha").

7. ARGUMENT

§102 REJECTION OF CLAIMS

THE APPLICABLE LAW

Anticipation requires the disclosure in a single prior art reference of each element of the claim under consideration, *In re Dillon.*[1] Anticipation also requires the presence in a single prior reference disclosure of each and every element of the claimed invention, *arranged as in the claim, Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*[2]

REJECTION OF CLAIMS 1-6, 31-36, AND 40 UNDER §102(B) AS BEING ANTICIPATED BY TROSTLE IS CLEARLY NOT PROPER AND WITHOUT BASIS BECAUSE TROSTLE DOES NOT DISCLOSE EVERY ELEMENT OF THE REJECTED CLAIMS

Claims 1-6, 31-36 and 40 were rejected under 35 U.S.C. § 102(b) for anticipation by Trostle (U.S. 5,919,257). Anticipation requires the disclosure in a single prior art reference of e element of the claim under consideration, *In re Dillon.*[3]

Concerning independent claims 1, 31, 32, 33, and 40:

Appellants believe that the issue of the patentability of independent claims 1, 31, 32, 33, and 40 over Trostle is best understood with regard to independent claim 1.

---

[1] 919 F.2d 688, 16 USPQ2d 1897, 1908 (Fed. Cir. 1990) (en banc), cert. denied, 500 U.S. 904 (1991).
[2] 730 F.2d 1452, 221 USPQ 481, 485 (Fed. Cir. 1984) (citing *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 220 USPQ 193 (Fed. Cir. 1983))
[3] 919 F.2d 688, 16 USPQ2d 1897, 1908 (Fed. Cir. 1990) (en banc), cert. denied, 500 U.S. 904 (1991).

Independent claim 1 includes the following limitations:

causing a first identifier associated with a first user identity to be stored on a machine responsive to a first sales-related event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and

detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine.

In the Final Office Action dated February 14, 2008, the Examiner contends that the foregoing limitations of independent claim 1 are disclosed by Trostle in col. 5, lines 45 – 67.

Trostle recites:

***FIG. 5** is a flow chart illustration of the login process based upon NDS authentication employed in NetWare 4.1. In step 82, a username prompt is presented to the user. In response, the user enters a username, which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends. However, if the entered username is on the list, the server returns an encrypted private key to the workstation in step 88. The encrypted private key can only be decrypted with the user's password. In step 90 the server checks if any login restrictions, such as time restrictions, station restrictions, and account lockout restrictions have been violated. These restrictions prevent logins from unauthorized workstations or logins during the wrong time of day. If there are violations, access is denied (step 86). However, if there are no login restrictions, the user is prompted to enter a password in step 92 and the validity of password is determined in step 94*[4]

Thus, Trostle relates to a two-step login process of user identification. First, a user is prompted to enter his username. (Note that the username was not stored on the machine.) The username is then transmitted to the server and validated against a list of the authorized usernames. If the username is not among the authorized usernames, the access is denied. . Thus, the login process proposed in Trostle denies access based on the determination that the user id is not authorized.

[4] Trostle, col 5, lines 45-67

In contrast to Trostle, independent claim 1 requires *detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity.* It must also be noted that it is this *machine which is coupled to the network-based transaction facility via a network.* Thus, the first identifier is stored on the client machine not the server system. In Trostle, there is no username stored on the client machine, that user name is entered by the user. In Trostle, the server does have a list of authorized usernames, however, that is the portion that matches with the *network-based transaction facility* feature in the claim not the machine. Since the Trostle reference does not disclose storing an identifier on a client machine, the Trostle reference fails to anticipate the claimed invention.

Furthermore, in order to detect *potentially fraudulent activities*, independent claim 1 requires "***a first user identity***" and "***a second user identity***" whereas Trostle is merely concerned with whether a single username is among the "authorized users". Thus, it is clear that Trestle cannot be reasonably characterized as disclosing "*a first user identity*" and "*a second user identity*" cited by independent claim 1.

Additionally, independent claim 1 requires "*detecting a* ***lack of correspondence between the first identifier stored on the machine and a second identifier*** *associated with a second user identity.* Because there is Trostle is concerned with a single username, Trostle cannot be reasonably characterized as detecting a lack of correspondence between "*a first user identity*" and "*a second user identity*".

Accordingly, for at least the reasons stated above, Trostle fails to disclose all limitations of independent claim 1, and therefore the rejection of claims 1, 31, 32, 33, and 40 as anticipated by Trostle is improper and should be withdrawn.

Concerning claims 2-6 and 34-36:

Appellants respectfully submit that claims 2-6 and 34-36 depend directly or indirectly from independent claims 1 and 33. As such, these dependent claims incorporate all the limitations of their parent independent claims. Accordingly, Appellants submit that these dependent claims are patentable for at least the reasons set forth above.

Thus, Appellants respectfully request withdrawal of the rejections of claims 2-6 and 34-36. For brevity, Appellants reserve the right to present further remarks concerning the patentable distinctiveness of such dependent claims.

§103 REJECTION OF CLAIMS

THE APPLICABLE LAW

The test for obviousness is what the combined teachings of the references would have suggested to one of ordinary skill in the art. In re Young[5]. Moreover, in evaluating such references it is proper to take into account not only the specific teachings of the references but also the inferences, which one skilled in the art would reasonably be expected to draw therefrom. In re Preda[6]. Thus, what is required in the analysis is "some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" and not "precise teachings directed to the specific subject matter of the challenged claim" when inferences and creative steps that a person of ordinary skill in the art would employ are taken into consideration[7]. KSR Int'l Co. v. Teleflex Inc.

REJECTION OF CLAIMS 7- 9, 19-20, 30, AND 37- 40 UNDER §103 AS BEING UNPATENTABLE OVER PRIOR ART IS CLEARLY NOT PROPER AND WITHOUT BASIS BECAUSE THE FINAL OFFICE ACTION DID NOT EXPLAIN WHY THE DIFFERENCES BETWEEN THE PRIOR ART AND THE REJECTED CLAIMS WOULD HAVE BEEN OBVIOUS TO ONE OF ORDINARY SKILL IN THE ART

Claims 7-8 and 37 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Trostle in view of Buchner et al. (Discovering Internet marketing intelligence through online

[5] 927 F.2d 588,591,18 USPQ2d 1089, 1091 (Fed. Cir. 1991) and In re Keller, 642 F.2d 413,425,208 USPQ 87 1, 881 (CCPA 1981)
[6] 401 F.2d 825,826, 159 USPQ 342,344 (CCPA 1968)
[7] 127 S. Ct. 1727,82 USPQ2d 1385,1396 (2007)

analytical web usage mining, ACM SIGMOD Record archive, Vol. 27, Issue 4, (December 1998), Pages: 51-61), hereinafter Buchner. Claims 9-19 and 38 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Trostle in view of Buchner as applied to claims 8 and 37 above, and further in view of Miller (Michael Miller, The complete Idiot's Guide to Ebay Online Auctions, copyright July 1999). Claims 20-30 and 39 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Trostle in view of Buchner and Miller as applied to claims 19 and 38 above, and in further view of Smaha et al (U.S. 5,557,742), hereinafter Smaha. Appellants respectfully traverse these rejections.

Appellants have argued above that Trostle fails to disclose elements of independent claims 1, and 33 from which dependent claims 7- 9, 19-20, 30, and 37- 40 depend either directly or indirectly. The Final Office Action alleges that Buchner, Miller, and Smaha teach certain additional elements but is silent as to why Trostle, Buchner, Miller, and Smaha when combined would teach or suggest elements that Appellants argued above as lacking in Trostle. Neither does the Final Office Action explain why the differences between the combination of Trostle, Buchner, Miller, and Smaha and the rejected claims would render the rejected claims obvious to one of ordinary skill in the art. Appellants have carefully reviewed Buchner, Miller, and Smaha but found no language teaching what is lacking in Trostle either on its own or in combination with Trostle. Accordingly, Appellants respectfully request that the obviousness rejection of claims 7- 9, 19-20, 30, and 37- 40 be withdrawn.

SUMMARY

At least for the reasons argued above, claims 1-6, 31-36, and 40 were not properly rejected under 35 U.S.C. § 102(b) for anticipation by Trostle. Additionally, at least for the reasons argued above, claims 7-30 and 37-39 were not properly rejected under 35 U.S.C. § 103(a) as being unpatentable over combinations of Trostle, Buchner, Miller, and Smaha. It is respectfully submitted that the references cited do not render the claims anticipated or obvious and that the claims are patentable over the cited references. Reversal of the rejections and allowance of the pending claims are respectfully requested.

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. Box 2938
Minneapolis, MN 55402

Date October 10, 2008 By

Georgiy L. Khayet
Reg. No. 59,595

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 10 day of October 2008.

Name

Signature

8. CLAIMS APPENDIX

Claims 1 - 40, as of February 14, 2008 (Date of Final Office Action).

1. A method to detect fraudulent activities at a network-based transaction facility, the method comprising:

causing a first identifier associated with a first user identity to be stored on a machine responsive to a first sales-related event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and

detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine.

2. A method as in claim 1 comprising causing the second identifier to be stored on the machine in responsive to the second sales-related event.

3. A method as in claim 2 comprising causing the lack of correspondence between the first identifier and second identifier to be detected at the machine.

4. A method as in claim 3 comprising receiving both the first identifier and the second identifier at the network-based transaction facility from the machine, and detecting the lack of correspondence between the first identifier and second identifier at the network-based transaction facility.

5. A method as in claim 4 comprising recording of the potentially fraudulent activity at the network-based transaction facility responsive to a detection of the lack of correspondence between the first identifier and the second identifier.

6. A method as in claim 5 wherein the second sales-related event is a sales transaction event, the method further comprising prohibiting a completion of the sales transaction event responsive to the detection of the lack of correspondence between the first identifier and the second identifier.

7. A method as in claim 6 comprising causing the first identifier to be stored on the machine within a cookie.

8. A method as in claim 7 comprising causing the first identifier and the second identifier to be recorded with the cookie.

9. A method as in claim 8 wherein the first sales-related event includes one of registering with the network-based transaction facility, communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility, communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility.

10. A method as in claim 9 wherein the sales transaction event includes one of registering with the network-based transaction facility, communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility , communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility.

11. A method as in claim 10 comprising:

causing the first identifier and the second identifier to be stored on the machine with a shill cookie;

causing a cookie identifier to be stored with the shill cookie;

causing the shill cookie to be coupled to a cookie bundle which records a plurality of transaction preferences for the first user identity and the second user identity on the machine;

causing the shill cookie bundle to be sent from the machine to the network-based transaction facility when the second user identify makes the second sales transaction event with the network-based transaction facility using the machine;

causing the shill cookie to be appended with the second identifier responsive to the detection of the lack of correspondence between the first identifier and the second identifier at one of the machine and the network-based transaction facility;

causing the cookie bundle to be inspected for the potentially fraudulent activity; and

causing the potentially fraudulent activity to be recorded into a database.

12. A method as in claim 11 wherein an inspection of the shill cookie comprises a source for the detection of the lack of correspondence between the first identifier and the second identifier.

13. A method as in claim 12 further comprising:

causing the cookie bundle to be a non-session cookie residing on the machine for a predetermined amount of time.

14. A method as in claim 13 further comprising:

causing the shill cookie to be appended every time a new user identifier is used to establish a new event with the network-based transaction facility using the machine wherein there is a lack of correspondence between the new user identifier and the first user identifier.

15. A method as in claim 14 wherein the machine comprises a computer connected to the network-based transaction facility.

16. A method as in claim 15 wherein the network-based transaction facility comprises an Internet-based auction facility.

17. A method as in claim 16 further comprising:

causing the shill cookie to record and to store a predetermined number of user identifiers.

18. A method as in claim 17 further comprising causing the shill cookie and the cookie bundle to be encoded such that the shill cookie and the bundle cookie are coded.

19. A method as in claim 18 further comprising causing the shill cookie and the cookie bundle to be encrypted.

20. A method as in claim 19 further comprising:

generating a potential fraudulent activities table having a fraudulent activity field, a cookie identifier field, a user identifier field, and a frequency field;

recording each of the potentially fraudulent activities and corresponding information into the potential fraudulent activities table;

updating the potential fraudulent activities table at least on a periodic basis; and

providing an updated report of the potential fraudulent activities table to an investigation team

21. A method as in claim 20 further comprising:

configuring the potential fraudulent activities table to include a transaction product category field, a transaction country field, a transaction price range field, and a transaction activity field.

22. A method as in claim 21 wherein the new event includes one of registering with the network-based transaction facility, communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility, communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility.

23. A method as in claim 22 further comprising providing the updated report to the investigation team at a predetermined time.

24. A method as in claim 23 further comprising providing the network-based transaction facility with a capability to override the updated report to the investigation team as necessary.

25. A method as in claim 24 further comprising providing a priority ranking system having a low priority for a low potential fraudulent activity frequency, a medium priority for a medium potential fraudulent activity frequency and a high priority for a high potential fraudulent activity frequency.

26. A method as in claim 25 further comprising examining the updated report to confirm the potentially fraudulent activity.

27. A method as in claim 26 wherein the potentially fraudulent activity includes one of shill biddings and shill feedbacks.

28. A method as in claim 27 wherein the recording does not affect any one of the first sales-related event, the second sales-related event, and the new event.

29. A method as in claim 28 further comprising causing the detection of the potentially fraudulent activity responsive a matching of at least two user transaction preferences from at least two different user identifies.

30. A method as in claim 29 wherein the user transaction preferences comprise credit card numbers, bidding histories, payment methods, and shipping addresses.

31. A computer readable medium comprising instructions, which when executed on a processor, cause the processor to perform a method for detecting suspicious transactions made over a network-based transaction facility using a client machine, the method comprising:

causing a first identifier associated with a first user identity to be stored on a machine responsive to a first sales-related event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and

detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine.

32. A method for detecting suspicious transactions made with an Internet service facility from one computerized facility, the method comprising:

causing a first identifier associated with a first user identity to be stored on a machine, the causing being responsive to a first sales-related event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and

detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity, the detecting being responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine.

33. A system to detect fraudulent activities at a network-based transaction facility, the system comprising:

an identifier processor to cause a first identifier associated with a first user identity to be stored on a machine responsive to a first sales-related event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and

a first detection processor to detect a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine.

34. A system as in claim 33 comprising a second detection processor to cause the lack of correspondence between the first identifier and second identifier to be detected at the machine.

35. A system as in claim 34, said second detection processor to receive both the first identifier and the second identifier at the network-based transaction facility from the machine, and to detect the lack of correspondence between the first identifier and second identifier at the network-based transaction facility.

36. A system as in claim 35 comprising a first recording processor to record the potentially fraudulent activity at the network-based transaction facility responsive to a detection of the lack of correspondence between the first identifier and the second identifier.

37. A system as in claim 36 comprising a cookie recording processor to record the first identifier and the second identifier to be recorded within a cookie.

38. A system as in claim 37 comprising:

a storing processor to cause the first identifier and the second identifier to be stored on the machine within a shill cookie and a cookie identifier to be stored within the shill cookie;

a bundling processor to cause the shill cookie to be coupled to a cookie bundle which records a plurality of transaction preferences for the first user identity and the second user identity on the machine;

a sending processor to cause the shill cookie bundle to be sent from the machine to the network-based transaction facility when the second user identify makes the second sales transaction event with the network-based transaction facility using the machine;

an appending processor to cause the shill cookie to be appended with the second identifier responsive to the detection of the lack of correspondence between the first identifier and the second identifier at one of the machine and the network-based transaction facility;

an inspection processor to cause the cookie bundle to be inspected for the potentially fraudulent activity; and

a second recording processor to cause the potentially fraudulent activity to be recorded into a database.

39. A system as in claim 38 further comprising:

a tabulating processor to generate a potential fraudulent activities table having a fraudulent activity field, a cookie identifier field, a user identifier field, and a frequency field;

a third recording processor to record each of the potentially fraudulent activities and corresponding information into the potential fraudulent activities table;

an updating processor to update the potential fraudulent activities table at least on a periodic basis and to provide an updated report of the potential fraudulent activities table to an investigation team.

40. A system to detect fraudulent activities at a network-based transaction facility, the system comprising:

a first means for causing a first identifier associated with a first user identity to be stored on a machine responsive to a first sales-related event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and

a second means for detecting a potentially fraudulent activity by detecting a lack of correspondence between the first identifier stored on the machine and a second identifier associated with a second user identity responsive to a second sales-related event with respect to the network-based transaction facility and initiated under the second user identity from the machine.

9. EVIDENCE APPENDIX

None.

10. RELATED PROCEEDINGS APPENDIX

None.